Optical resources for highly secure remote object authentication

María S. Millán[1a], Elisabet Pérez-Cabré[a], Bahram Javidi[b]
[a]Dept. Optica i Optometria, Universitat Politècnica de Catalunya, Terrassa, Spain;
[b]Electrical & Computer Engineering Dept., University of Connecticut, 371 Fairfield Road, Unit 2157, Storrs, CT 06269-2157, USA.

ABSTRACT

We review the potential of optical techniques in security tasks and propose to combine some of them in automatic authentication. More specifically, we propose to combine visible and near infrared imaging, optical decryption, distortion-invariant ID tags, optoelectronic devices, coherent image processor, optical correlation, and multiple authenticators. A variety of images and signatures, including biometric and random sequences, can be combined in an optical ID tag for multifactor identification. Encryption of the information codified in the ID tag allows increasing security and deters from unauthorized usage of optical tags. The identification process encompasses several steps such as detection, information decoding and verification which are all detailed in this work. Design of rotation and scale invariant ID tags is taken into account to achieve a correct authentication even if the ID tag is captured in different positions. Resistance to some noise and degradation of the tag is analyzed. Examples and experiments are provided and the results discussed.

Keywords: Information security, optical ID tags, pattern recognition, multifactor validation, near infrared imaging

1. INTRODUCTION

Complex operations such as authenticator selection, signature encoding, encryption, identity tags, remote readout, decryption, hybrid processors, pattern recognition, resistance to degradations, identification, (multifactor) validation, and authentication are involved in the broad area of security systems. Optics provides useful resources for remote, real-time, automatic and reliable signal verification as it has been reported by a large number of papers published in the last decades.[1-3]A method to encode a primary image into a white-noise-like distribution is proposed in Ref. [4] and it can be implemented either optically or electronically. It has been applied to identify objects by optical correlation[5] in a nonlinear joint-transform correlator (JTC).[6] In nonlinear (fully-phase) encoding, a phase-only version of the primary image is encoded.[7] The identity (ID) tags consist of an optical code containing complex valued encrypted information to increase security.[8] A distortion-invariant ID tag,[9] was designed so that the verification system was able to detect and identify the information included in the tag even when the optical code was captured rotated or at a varying distance. Other optical techniques have been used in the field of security systems, for instance, to multiplex encrypted data by polarized light,[10] or to encrypt three-dimensional information with digital holography.[11]

In this work, we want to make the system more secure by synthesizing signatures from different spectral bands (VIS and NIR images) or by using multifactor authenticators. The encrypted information included in the distortion-invariant ID tag is verified by comparing the decoded signal with a reference signature. In the steps of the procedure we show the benefits of using combined optical and digital image processing techniques implemented by optoelectronic systems.

2. SELECTION OF AUTHENTICATORS

So far, optical security techniques deal with a single primary image (an object, a signature, or a biometric signal) as authenticator. However, security can be reinforced by combining different authenticators. In such a case, a Boolean AND operation has to be performed for each factor's authentication results so all must be affirmative before final authentication is satisfied.[12] The selection of authenticators is a crucial step because the identification of an element (object or person or both) is based on them. They must uniquely represent the element whose identity is to be validated on a basis of signal recognition. Frequently, the authenticators are images such as logotypes, bar codes, alphanumerical

1 millan@oo.upc.edu; phone 34 93 7398339; fax 34 93 7398301; www.goapi.upc.edu

Applications of Digital Image Processing XXX, edited by Andrew G. Tescher
Proc. of SPIE Vol. 6696, 66961P, (2007) · 0277-786X/07/$18 · doi: 10.1117/12.738338

signs, signatures, biometric information, and random sequences. A possibility is to combine information coming from different spectral bands, for instance, the VIS and NIR bands. Infrared data have already been used for target detection in security systems.[13] This method takes advantage of the different spectral reflectance of objects in VIS and NIR bandwidths. Regarding the signals, biometric images such as fingerprints, face, hand, iris, retina, etc. are more and more considered in authentication mechanisms because biometrics is based on something intrinsic to a person (something the person is) in contrast to other schemes based on either something a person knows (e.g. a password) or has (e.g. a metal key, an ID card).[12]

In this work we consider multiple signals to identify a person, an object or both. The information is combined using two different techniques: in the first technique, a single signature is synthesized from two signals in the VIS and NIR spectral bands.[14] Secondly, we use a multifactor encryption-authentication technique that reinforces optical security by allowing the simultaneous AND-verification of four primary images.[15] These optical techniques are attractive for high-security purposes that require multiple reliable authentications.

2.1 Single signature synthesized from VIS and NIR images

We describe this technique using the images shown in Fig. 1 (Example 1). For instance, as reference signature we consider a numerical code reproduced by printing a sheet of paper by using two different types of ink, commonly used in commercially available printers. The sheet has a white part and a black part. The complete signature results from the synthesis of captured data from the VIS and NIR spectral bands. Fig. 1(a) displays the intensity distribution of the captured image, $f_{VIS}(x)$ in one-dimensional notation for simplicity, when the signature is illuminated by daylight and captured by a conventional camera sensitive to the visible spectral bandwidth (VIS-camera). Only information at the bottom part of the signature is recognizable from the visible image. Fig. 1(b) shows the corresponding captured image, $f_{NIR}(x)$, when the signature is illuminated by a set of LEDs emitting in the near infrared region (for example, around 950 nm) and captured by a camera sensitive to this spectral region (NIR-camera). In the NIR channel, only the upper half of the signature is reproduced. Binarized versions of both the VIS and the NIR images ($\overline{f}_{VIS}(x)$, $\overline{f}_{NIR}(x)$) can be combined by using the logical operation

$$f(x) = \left\{ NOT\left[\overline{f}_{VIS}(x) \right] \right\} XOR \left\{ \overline{f}_{NIR}(x) \right\}, \tag{1}$$

which is computed to obtain the whole numerical code acting as the signature (Fig. 1(c)). The two parts of this synthesized signature could represent the passwords that reveal the identities of two elements, for instance, a vehicle and its driver. From the whole numerical code $f(x)$ of Fig. 1(c), the encrypted signal $\psi(x)$ is to be computed in Section 3.

(a) $f_{VIS}(x)$ (b) $f_{NIR}(x)$ (c) $f(x)$

Fig. 1. Example 1: (a) VIS image and (b) NIR image that compose the reference signature. (c) Synthesized signature that results from applying Eq. (1) to the binarized versions of VIS and NIR images.

2.2 Biometrics and multifactor authenticators

The technique presented here is designed for four-factor authentication.[15] There is no a priori constraint about the type of primary images to encode. In Example 2 (Fig. 2) a combination of one biometric (to validate the authorised person), one alphanumeric sign and one pattern (to validate a vehicle) and one random phase sequence (to act as key code) are considered. The vessel distribution of a retina fundus image, which is stable, accurate, and very effective information for authentication, is used as biometric signal. The key phase code is known by the database of the authentication processor and is introduced as a degree of freedom to codify, for instance, the key of the day. These four reference primary images, double-phase encoded (see Section 3) and encrypted in an ID tag (see Section 4), are compared with the actual input images obtained *in situ* from the person and the vehicle whose authentication is wanted.

(a) Biometric $s(x)$ (b) Tyre pattern $r(x)$ (c) Key code $b(x)$ (d) Vehicle plate $n(x)$

Fig. 2. Example 2. Reference primary images to consider as multiple authenticators in the multifactor encryption-authentication technique.

3. COMPLEX-AMPLITUDE ENCRYPTED FUNCTION $\psi(x)$

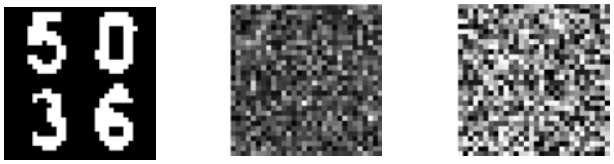
3.1 Fully-phase encrypted function $\psi^s(x)$ of a single signature

Let $f(x)$ be the signature to be encrypted that is a normalized positive function distributed in [0,1] and has a total amount of pixels N. This image can be phase-encoded to yield $t_f(x)$ that is generically defined by $t_f(x)=\exp\{j\pi f(x)\}$. The coordinates in the spatial and in the frequency domain are represented by (x) and (μ), respectively. Similarly to the double-phase encoding,[4] the fully-phase encryption technique[7] converts a primary image $f(x)$ into stationary white noise, so that the encrypted function does not reveal the appearance of the signature to the naked eye. The signature to be encoded is represented as a phase-only function by computing $t_f(x)$. The range of variation of the phase encoding is $[0,\pi]$. Afterwards, the phase-encoded image is multiplied by the phase mask $t_{2p}(x)=\exp\{j2\pi p(x)\}$. Finally, this product is convolved by a function $h(x)$, which is the impulse response of a phase-only transfer function $H(\mu)=t_{2b}(\mu)=\exp[j2\pi b(\mu)]$. Thus, the fully phase encrypted function $\psi^s(x)$ is a complex valued function given by

$$\psi^s(x)=t_{f+2p}(x)*h(x). \tag{2}$$

Fig. 3 shows the magnitude and phase distributions of the encrypted function $\psi^s(x)$ obtained when Eq. (2) is applied to the original synthesized signature of Example 1 (Fig.1(c)). It can be seen that the dim appearance of the encrypted function does not reveal the content of the original signature.

To decrypt the information included in the encrypted function $\psi^s(x)$, it will be necessary to firstly Fourier transform and multiply by the complex conjugate of the phase mask, or key 1, used in the encryption procedure, $t_{-2b}(\mu)$. The output $t_{f+2p}(x)$ is obtained. The original signature is retrieved in the space domain by using a second key, $t_{-2p}(x)$, extracting the phase of $t_f(x)$ and dividing by π.



(a) $f(x)$ (b) $|\psi^s(x)|$ (c) $\phi_{\psi^s}(x)$

Fig. 3. (a) Signature synthesized from the binarized versions of VIS and NIR images (Example 1, Fig.1) (b) Magnitude and (c) Phase distributions of the fully phase encrypted function $\psi^s(x)$ that results from applying Eq. (2) to (a).

3.2 Fully-phase encrypted function $\psi^m(x)$ of multifactor signatures

Let $r(x)$, $s(x)$, $b(x)$, and $n(x)$ be the multiple authenticators or reference primary images (for instance, those of Example 2 in Fig. 2), in one-dimensional notation for simplicity. As in the previous case (Section 3.1), all the four primary images $r(x)$, $s(x)$, $b(x)$ and $n(x)$ are normalized positive functions distributed in [0,1]. These images can be phase-encoded to yield $t_r(x)$, $t_s(x)$, $t_{2b}(x)$, $t_n(x)$ that are generically defined by $t_f(x)=\exp\{j\pi f(x)\}$. The fully-phase encrypted function containing the multifactor authenticators is given by the equation

$$\psi^m(x) = t_{r+2b}(x) * t_s(x) * \mathbb{F}^{-1}\left[t_n(x)\right], \tag{3}$$

where $t_{r+2b}(x) = t_r(x)\, t_{2b}(x) = \exp\{j\pi r(x)\}\exp\{j2\pi b(x)\}$, $\mathbb{F}^{-1}$ indicates inverse Fourier transform, and $*$ the convolution operation. The encrypted function is complex-amplitude valued. It can be either optically generated by using an optical hardware equivalent to a JTC or computed and electronically implemented using conventional techniques for computer generated holograms.

Fig. 4 shows the magnitude and phase distributions of the encrypted function $\psi^m(x)$ obtained when Eq. (3) is applied to the set of reference primary images of Example 2 (Fig.2). Again, the appearance of the encrypted function is dim enough and does not reveal the content of any primary image of the set. The specific combination of information expressed by Eq. (3) is related to the automatic process of optical simultaneous recognition to validate the set of four authenticators. It will be all described and justified in Section 6.

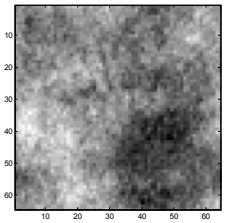
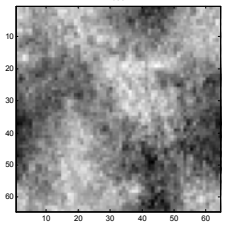
Magnitude $\left|\psi^m(x)\right|$  Phase $\phi_{\psi^m}(x)$ 

Fig. 4. Magnitude and phase distributions of the fully phase encrypted function $\psi^m(x)$ that results from applying Eq. (3) to the set of reference primary images of Example 2 (Fig.2).

4. ID TAG RESISTANT TO NOISE, SCALE AND ROTATION DISTORTIONS

A robust ID tag must include the information of the encrypted function in a way that it can be read with invariance to certain distortions, in particular, to scale variations and rotations. If this property is shown, the receiver will be able to remotely capture the ID tag from an unexpected location and orientation and, within certain limits, to successfully process the information included in it. We follow the procedure described in Ref. 16. Distortion-invariance is achieved by both multiplexing the information included in the ID tag and taking advantage of the ID tag topology.

The complex valued encrypted function $\psi(x)$, which represents either $\psi^s(x)$ or $\psi^m(x)$ of Section 3 in general, is to be fully grayscale encoded. Let us consider the $\psi(x)$ in array notation $\psi(t) = |\psi(t)|\exp\{i\phi_\psi(t)\}$ where t=1,2,...N, and N is the total number of pixels of the encrypted function. We build two vectors: the magnitude vector $|\psi(t)|$ and the phase vector $\phi_\psi(t)$, with t=1,2,...N. The information included in the ID tag is distributed in two circles. Fig. 5 shows a possible arrangement of both circles. One of the circles corresponds to the magnitude $|\psi(t)|$ of the encrypted signature (left circle in Fig. 5). The other contains the phase distribution $\phi_\psi(t)$ of the encrypted function (right circle in Fig. 5). In both circles, the information is distributed similarly to the structure of a wedge-ring detector. One half of each circle (upper semicircles in Fig. 5) includes either the magnitude or the phase distribution of the encrypted function written in a radial direction and repeated angularly so that rotation-invariance can be achieved. The other semicircle of both circles (bottom semicircles in Fig. 5) contains either the magnitude or the phase distribution of the encrypted function written circularly and repeated in concentric rings. Therefore, the information of a given pixel of the encrypted function will correspond to an angular sector in the optical code. Thus, the readout of the ciphered information will be tolerant to variations in scale. For encrypted signatures with a large number of pixels, such as the examples given in Section 3, information of the

scale-invariant ID tag have to be distributed by using different concentric semicircles to assure a minimum number of pixels for each sector to recover the information properly. Consequently, the tolerance to scale variation will be affected in accordance to the number of concentric circles used in the ID tag. Fig. 6 shows the ID tag corresponding to the encrypted function of Fig. 3 (b,c).

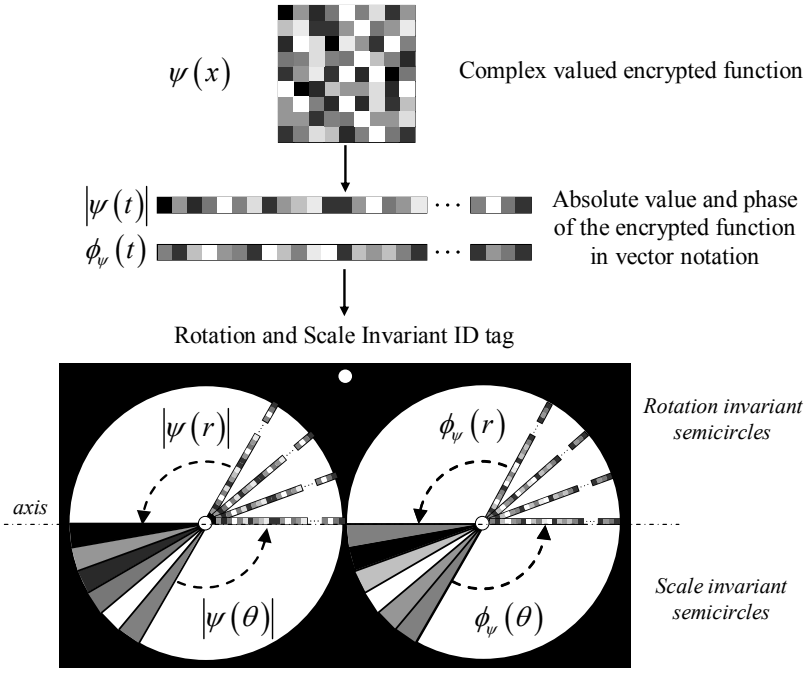


Fig. 5. Synthesis of a rotation and scale invariant ID tag from the encrypted function $\psi(x)$.

As it is shown in Fig. 5, the centers of both circles are white dots that, along with a third white dot in the upper part, build a reference triangular shaped pattern that allows one to know the orientation of the whole ID tag. Both, the magnitude $|\psi(t)|$ and the phase $\phi_\psi(t)$ are encoded in grayscale in the left and right circles, respectively. Other possibilities can be considered to rearrange the information contained in the two circles of the ID tags.[17] The choice of a particular distribution of the signal information depends on practical considerations of a given problem. Using the procedure described, the information is also redundantly written, so that an improved resistance to noise and other damages due to common handling (e.g. scratches) is obtained.

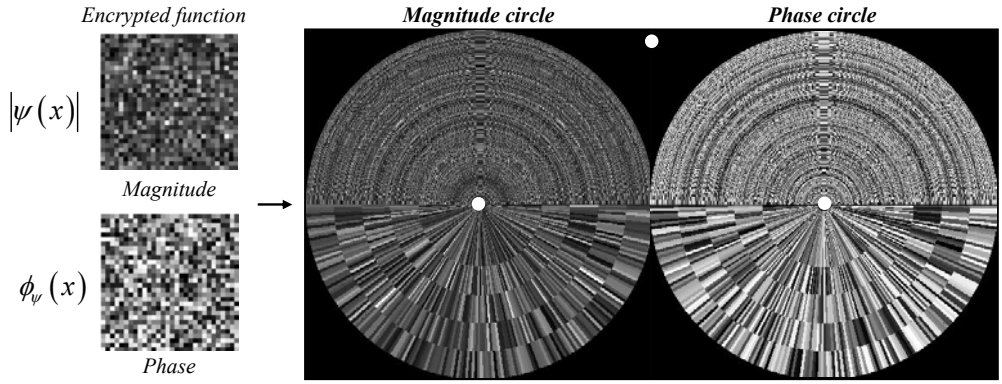


Fig. 6. Rotation and scale-invariant ID tag corresponding to the signature of Fig.3.

5. REMOTE READOUT AND DECODIFICATION

The ID tag can be captured in a situation similar to that represented in Fig. 7. The information contained in the ID tag stuck on the vehicle has to be compared with the input signals contained, for instance, in a card. In this way, it is possible to verify the identity of both the card holder and the vehicle. When the ID tag is captured, the encrypted information is decoded following a deciphering procedure that is the reverse of that described in Section 4. From one circle the magnitude is obtained and from the other, the phase distribution. Once the border between the rotation-invariant area and scale-invariant area is extracted (the axis in Fig. 8), the signature in vector notation $\psi(t)$ can be decoded either from the rotation or the scale-invariant region. From the rotation-invariant region, the optical code can be read out by using a linear array detector placed in any radius of the semicircle, from the center to the exterior of the code. Not only is a single code read along a unique radial direction for decoding, but a median value from several radial codes is computed to increase robustness against noise. Pixels are written back into matrix notation prior to dechiphering the signature $\psi(x)$. Following this procedure, the encrypted signature will be recovered whether the ID tag is captured in its original orientation or its rotated format. Similarly, $\psi(t)$ can be recovered by reading the ID tag in circular rings in the scale-invariant region. To minimize errors in the reading process, the median value of pixels located in neighbour rings is computed. The signature is then written in matrix notation $\psi(x)$ and decrypted. The optical code will be recovered even if the ID tag is captured in its original size or scaled.

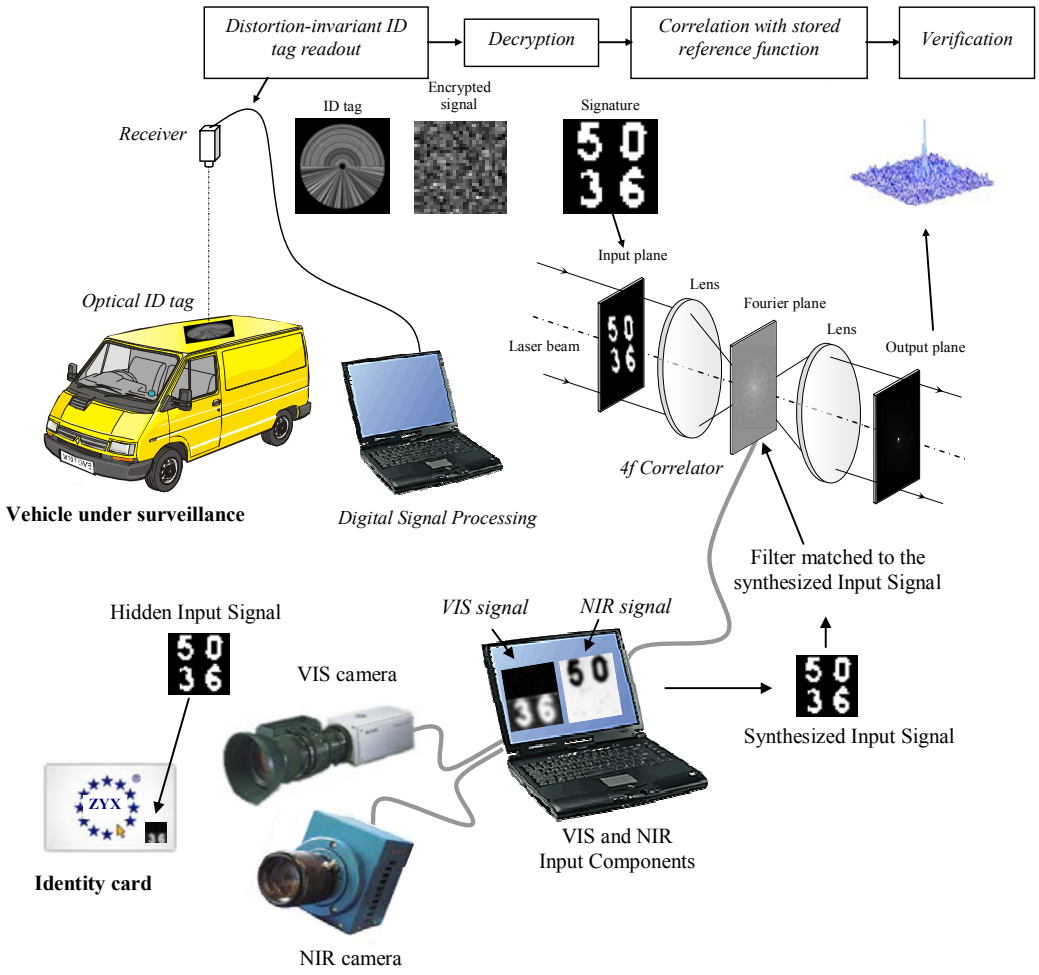


Fig. 7. Diagram of the ID tag readout, signature decryption and comparison with the input synthesized signal in an optical correlator for verification.

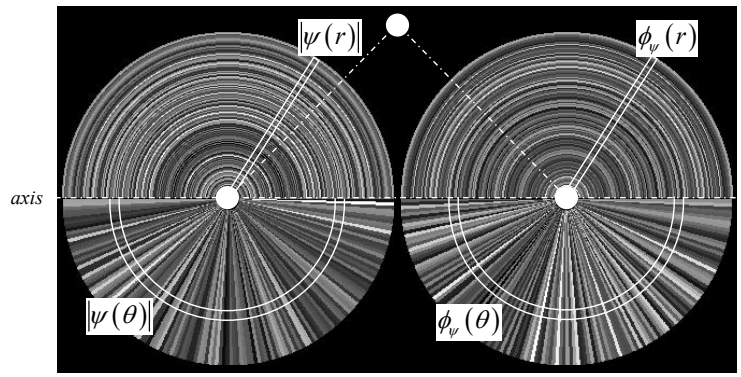


Fig. 8. Readout of the rotation and scale-invariant ID tag.

6. OPTICAL PROCESSOR FOR VERIFICATION

6.1 Of a single signature

The processor that verifies the information of the single signature contained in the ID tag can be an optical correlator.[5] Fig. 7 shows the classical *4f* setup for optical correlation. The signature to be verified is imaged onto the input plane, and compared with the synthesized input image obtained from the VIS and NIR imaging of an identity card. Another possibility is to compare the deciphered image of the ID tag with some stored reference function. A correlation-based processor[5] compares the decoded information with a reference signal. Comparison of these two functions is based on a nonlinear correlator.[18] Let $f(x)$ denote the decoded signal and $r(x)$ the reference signature. Let $|F(\mu)|$ and $|R(\mu)|$ be the modulus of their Fourier transforms, respectively, and let $\phi_F(\mu)$ and $\phi_R(\mu)$ denote their phase distributions in the frequency domain. The nonlinear correlation between the input and the reference signals is obtained by using the equation

$$c(x) = IFT\left\{\left|F(\mu)R(\mu)\right|^k \exp\left[j\left(\phi_F(\mu) - \phi_R(\mu)\right)\right]\right\} \tag{4}$$

where parameter k defines the strength of the applied nonlinearity.[18] We use k'th-law nonlinearity for computational efficiency. The nonlinearity determines the performance features of the processor, such as its discrimination capability, noise robustness, peak sharpness, etc. and it can be chosen according to the performance required for a given recognition task.[19] Correlation-based detection is feasible when an output peak above a noise floor is obtained. A threshold operation, applied to the correlation output, determines the identity of the object. The processor performance can be evaluated using different metrics.[20] We consider, as a measure of the system discrimination capability, the *cc*/*ac* metric, which is the ratio between the maximum peak value of the correlation output, *cc*, and the maximum autocorrelation value, *ac*, for the reference signature. Similarity between the decoded information and the reference signature will be great if the *cc*/*ac* ratio approaches the value of unity.

6.2 Of multifactor signature

The multifactor authentication technique involves an optical processor that consists of a combined nonlinear JTC and a classical *4f*-correlator[5] for simultaneous AND authentications of multiple images (Fig.9). We describe the principles of the method for a four-factor authentication taking into account that the encrypted function $\psi(x) = \psi^m(x)$, which has been decoded from the ID tag, was built according to Eq. (3).

Let $p(x), q(x), d(x)$, and $m(x)$, denote the positive and normalized input images to compare with the set of reference images, $r(x)$, $s(x)$, $b(x)$ and $n(x)$, respectively. In the first step, the ID tag $\psi(x-a)$ and one phase encoded input image, for instance $t_p(x+a) = \exp\{j\pi p(x+a)\}$, are displayed side-by-side a distance $2a$ apart on the input plane of the nonlinear JTC illuminated by coherent light (Fig. 9). The phase distribution $t_{2d}(x+a) = \exp\{j2\pi d(x+a)\}$ is placed

against the screen where the input $t_p(x+a)$ is displayed. Consequently, the amplitude distribution in the input plane is $\psi(x-a)+t_{p+2d}(x+a)$. A CCD sensor placed in the Fourier plane of the JTC captures the intensity distribution $\mathcal{I}(u)$ of the joint power spectrum,

$$\mathcal{I}(u)=\left|\mathbb{F}\left[\psi(x-a)+t_{p+2d}(x+a)\right]\right|^2. \tag{5}$$

The development of Eq. (5) gives the classical four terms of which two are interesting because they convey the cross-correlation signals that lead to spatially separated distributions in the output plane. These two terms are:

$$\begin{aligned}&\text{Term 1: } \mathbb{F}^*\left[\psi(x)\right]\mathbb{F}\left[t_{p+2d}(x)\right]\exp\{j2au\}=T^*_{r+2b}(u)T^*_s(u)t^*_n(u)T_{p+2d}(u)\exp\{j2au\},\\&\text{Term 2: } \mathbb{F}\left[\psi(x)\right]\mathbb{F}^*\left[t_{p+2d}(x)\right]\exp\{-j2au\}=T_{r+2b}(u)T_s(u)t_n(u)T^*_{p+2d}(u)\exp\{-j2au\},\end{aligned} \tag{6}$$

where a function in capital letter indicates the Fourier transform of the function in small letter and u is the spatial frequency coordinate. Terms 1 and 2 of Eqs. (6) can be modified according to a variety of nonlinear techniques. We consider nonlinear transformations of the joint power spectrum of the general form

$$NL^k\left\{\mathcal{I}(u)\right\}=\mathcal{I}(u)\left|\mathcal{I}(u)\right|^{k-1}, \tag{7}$$

where $k\in[0,1]$ defines the strength of the applied nonlinearity and it can vary from the linear case $(k=1)$ to the phase extraction technique[21] $(k=0)$ also called pure phase correlation[22] (PPC).

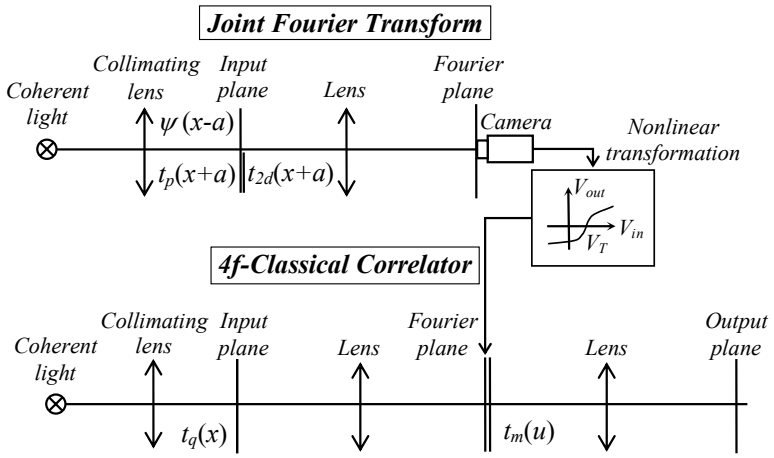


Fig. 9. Optical processor for multifactor authentication.

The resultant nonlinearly modified joint power spectrum (Eq. 7) is displayed on the Fourier plane of a 4f-classical correlator (Fig. 9). There, a transparency with the phase distribution $t_m(u)$ is placed against the screen. The input image $q(x)$ is phase encoded and displayed on the input plane of the 4f-correlator. Behind the Fourier plane, Terms 1 and 2 of Eqs. (3) are converted into:

$$\begin{aligned}&\text{Term 1: } \left[T_q(u)T^*_s(u)\left|T_s(u)\right|^{k-1}\right]\left[T^*_{r+2b}(u)T_{p+2d}(u)\left|T_{r+2b}(u)T_{p+2d}(u)\right|^{k-1}\right]\left[t^*_n(u)t_m(u)\right]\exp\{j2au\},\\&\text{Term 2: } \left[T_q(u)T_s(u)\left|T_s(u)\right|^{k-1}\right]\left[T_{r+2b}(u)T^*_{p+2d}(u)\left|T_{r+2b}(u)T_{p+2d}(u)\right|^{k-1}\right]\left[t_{n+m}(u)\right]\exp\{-j2au\}.\end{aligned} \tag{8}$$

If the information contained in the ID tag corresponds to a positive validation, then the multiple AND condition $r(x)=p(x)$ AND $s(x)=q(x)$ AND $b(x)=d(x)$ AND $n(x)=m(x)$ is fulfilled. In such a case, if the phase

extraction is applied $(k=0)$ and provided the system is free of noise and distortions, Term 1 of Eq. (8) simplifies into $|T_s(u)|\exp\{j2au\}$, which represents a wavefront with all its curvature cancelled[21] that focuses on a sharp multifactor autocorrelation peak centered in $x=-2a$ of the output plane (Fig. 1). From Eq. (8), the output intensity distribution corresponding to Term 1 is the cross-correlation of autocorrelation signals given by

$$\left|AC_{POF}\left[t_s(x)\right]\star AC^{*}_{PPC}\left[t_{r+2b}(x)\right]\star AC^{*}_{CMF}\left[T_n(x)\right]*\delta(x+2a)\right|^2, \tag{9}$$

where $\star$ denotes cross-correlation, and subindices CMF, POF, PPC indicate the sort of filter involved in the autocorrelation signal (CMF stands for classical matched filter, POF for phase-only filter, and PPC for pure phase correlation). Since autocorrelation peaks are usually sharp and narrow, particularly those for POF and PPC, we expect that the cross-correlation of such autocorrelation signals will be even sharper and narrower. Consequently, the information contained in Term 1, allows reinforced security verification by simultaneous multifactor authentication. On the other hand, when the multiple AND condition $r(x)=p(x)$ AND $s(x)=q(x)$ AND $b(x)=d(x)$ AND $n(x)=m(x)$ is fulfilled, and the phase extraction $k=0$ is considered, Term 2 of Eq. (8) becomes $\left[T_s^2(u)/|T_s(u)|\right]t_{2n}(u)\exp\{-j2au\}$, which does not yield any interesting result for recognition purposes. If $p(x)\neq r(x)$ or $q(x)\neq s(x)$ or $b(x)\neq d(x)$ or $n(x)\neq m(x)$, Term 1 contains a cross correlation signal that is, in general, broader and less intense than the multifactor autocorrelation peak of Eq. (9).

7. NUMERICAL EXPERIMENTS AND RESULTS

7.1 Single synthesized signature validation

Firstly, let us suppose that the receiver captures the ID tag, which should ideally contain two circles, one for the magnitude and the other for the phase to have the whole complex-amplitude of the encrypted function $\psi(x)$. Afterwards, the encrypted signature is deciphered and this information is compared with the reference synthesized signature $f(x)$ obtained from the combination of the VIS and NIR spectral components as it is computed by Eq. (1). The output signal of the processor for $k=0$ has its maximum intensity value (ac), which is normalized to unity (Fig. 10(a)), and a positive identification is achieved. Secondly, we consider that the distortion-invariant ID tag shown in Fig. 5 just contains the phase distribution of the encrypted signature, that is, the circle corresponding to $\phi_\psi(x)$. When the receiver captures the ID tag, the retrieved signature $\tilde{f}(x)$ can be compared with the signature read from the card $f_C(x)$. The fact that only the phase distribution is used makes the output peak intensity (cc) to decrease slightly but a positive and correct verification is still achieved in Fig. 10(b).

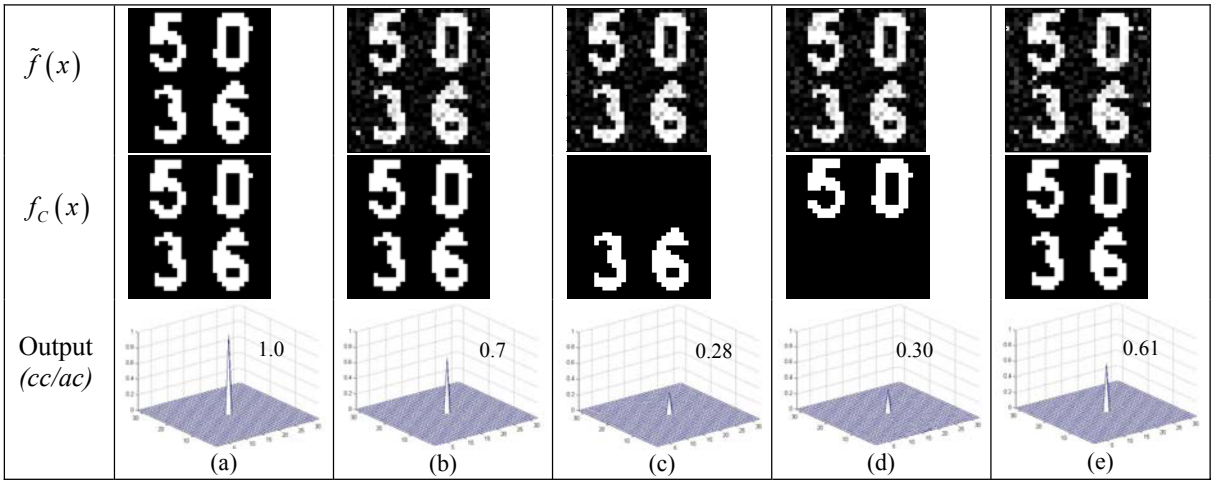


Fig. 10. Results of the single signature validation with *k*=0 (see the text and Fig. 7 for a reference).

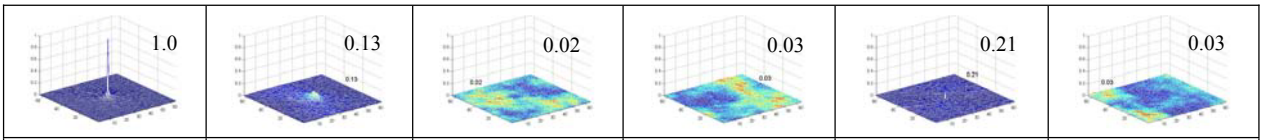
If the reference signature is only partially recovered by capturing a single spectral band (either the VIS or the NIR component), the system output is nearly null corresponding to a negative verification of the information (Figs. 10(c) and 10(d)). We tested the tolerance against rotation and scale variations of the image captured of the ID tag. Fig. 10(e) shows the results when the ID tag is captured under rotation of 60º degrees and x0.5 scaled. When the reference signature is correctly synthesized, the output peak reaches a high intensity value (over 0.5) that indicates a positive verification.

7.2 Multifactor validation

In Experiment 2, the set of input images can be equal to the reference set, partly different or totally different. Fig. 11 contains some input images, different from those reference primary images of Fig. 2, that are to be considered in the simulated experiments. In a preliminary part of the experiment, we compute the output intensity distribution corresponding to the Term 1 of the multifactor correlation with phase extraction (k=0). If the set of input images coincide with the set of reference primary images, then the result is given by Eq.(9). We compute and represent the normalised result in Fig. 12(a). It shows a sharp peak of intensity that allows a complete validation of the set of input images. In Fig. 12(b)-(e) we represent the results obtained when the input set of images differs from the reference set in just one image (specified at the bottom). Fig. 12(f) shows the result obtained when all the images of the input set are different from the respective reference images. All the results shown in Fig. 12 are very satisfactory: when the set of input images coincide with the reference set, a positive validation is obtained. But, when both sets are different, even for just one image, the output multicorrelation signal has no peak in general. These good results lead us to go on and encrypt function $\psi(x)$ in a rotation and scale invariant ID tag for remote authentication. To build the ID tag we consider binary and (32 x32 pixels) low resolution images (Fig. 13) that allow us to simplify the process and save computing time.

(a) Biometric $q(x)$ (b) Tyre pattern $p(x)$ (c) Key code $d(x)$ (d) Vehicle plate $m(x)$

Fig.11. Example 2. Input primary images to consider in the multifactor encryption-authentication experiment.



(a) Validation (b) $q(x) \neq s(x)$ (c) $p(x) \neq r(x)$ (d) $d(x) \neq b(x)$ (e) $m(x) \neq n(x)$ (f) None coincides

Fig. 12. Output intensities of Term 1 of the multifactor correlation with k=0. The images are in Fig.2 and Fig.11.

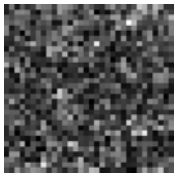
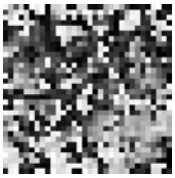
Reference primary images	Other images to compare	Function $\psi(x)$
$s(x)$ Biometric 	$q(x) \neq s(x)$ 	 $\lvert\psi^m(x)\rvert$
$r(x)$ Tyre pattern 	$p(x) \neq r(x)$ 	
$b(x)$ Random key code 	$d(x) \neq b(x)$ 	 $\phi_{\psi^m}(x)$
$n(x)$ Vehicle plate code 	$m(x) \neq n(x)$ 	

Fig. 13. Images to consider in the simulated experiments that involve encryption in the ID tag.

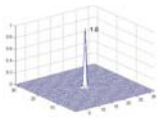
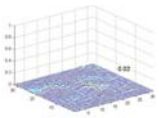
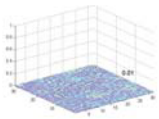
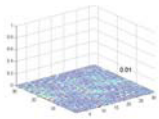
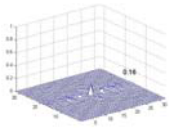
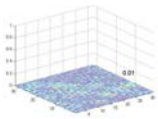
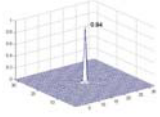
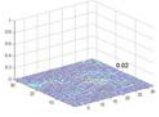
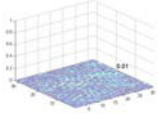
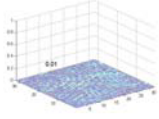
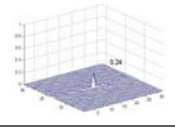
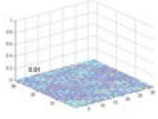
Validation	$q(x) \neq s(x)$	$p(x) \neq r(x)$	$d(x) \neq b(x)$	$m(x) \neq n(x)$	None coincides
Readout of the ID tag with no distortions by rotation or scale variations					
1.0 	0.02 	0.01 	0.01 	0.16 	0.01 
Readout of the ID tag with 60° rotation and 50% scaled					
0.94 	0.02 	0.01 	0.01 	0.24 	0.01 

Fig. 14. Output intensity distributions corresponding to the Term 1 of the multifactor correlation with phase extraction (k=0). The encoded function was retrieved from the decryption of the ID tag. The images considered are shown in Fig.13.

Once the complex valued encoded function $\psi(x)$ is computed, the rotation-scale invariant ID tag is built following the procedure of Fig. 5. The ID tags are read by the receiver and the encrypted function $\psi(x)$ is decoded. This function contains the reference primary images that are to be compared with a set of input images. Fig.14 shows the multicorrelation results in two situations: first, the readout of the ID tag is not affected by rotation or scaling, and second, the ID tag is read with 60º rotation and 50% scaled. It can be seen that validation is achieved in the correct case. When the input images do not match the reference set, total or partially, then the validation is denied. The effects of rotation or scaling are of little significance.

8. CONCLUSIONS

We have shown the potential of optical techniques in security tasks and have combined some of them in automatic authentication. We have used multiple signatures, distortion-invariant ID tags, optoelectronic devices, coherent image processor, optical decryption, optical correlation, and multiple authenticators. Neither the encrypted functions nor the ID tags reveal their content in any case, which is an extreme difficulty in counterfeiting. An intensity peak in the output plane of an optical processor will be used to decide whether an element (person or object) is authenticated or not. Authentication is achieved even if the ID tag is captured in its original position, scaled or rotated. The techniques described in this work can be useful to control the access to restricted areas, where the highly secure identification of a person, a vehicle or both is required.

We have proposed a highly secure single signature synthesized from VIS and NIR images that increases the system robustness against counterfeiting. Using only the phase circle of the ID tag, the encrypted function can be acceptably decoded and compared with the input synthesized signature in an optical correlator. Results provided by this technique show that only a proper synthesis of the VIS and NIR signals provides a positive verification. Tolerance to rotation and scale variations of the image captured from the ID tag has been demonstrated.

In a second technique, we encrypt multifactor authenticators in a single complex-amplitude function that can be used in combination with rotation-scale invariant ID tags. This optical technique is attractive for high-security purposes that require multifactor authentication and real-time automatic verification. It is advantageous to introduce nonlinearity in the optical signal processing by extracting the phase of the joint power spectrum. This modification leads to obtain sharp peaks of intensity in the output plane of the system that permit the multifactor authentication. We have presented the results obtained when the encrypted function is read and decoded from a rotation-scale invariant ID tag. In the studied cases, only the AND verification of the complete set of four signals led to the positive validation. Otherwise, if any mismatch appeared, the result was negative.

ACKNOWLEDGEMENTS

To the financial support of Spanish Ministerio de Educación y Ciencia and FEDER (project DPI2006-05479).

REFERENCES

1. B. Javidi, J.L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.* 33(6), 1752-1756 (1994).
2. J.L. Horner, B. Javidi, Opt. Eng. 38, Special issue on Optical security, 1999.
3. B. Javidi, *Optical and Digital Techniques for Information Security*, Springer, New York, 2005.
4. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* 20, 767-769 (1995).
5. J. W. Goodman, *Introduction to Fourier optics*, 2nd. Ed., McGraw Hill, New York, 1996.
6. B. Javidi, G. Zhang, J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," *Opt. Eng.* 35, 2506-2512 (1996).
7. N. Towghi, B. Javidi, Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Am.* A 16, 1915-1927 (1999).
8. B. Javidi, "Real-time remote identification and verification of objects using optical ID tags," *Opt. Eng.* 42, 1-3 (2003).
9. E. Pérez-Cabré, B. Javidi, "Scale and rotation-invariant ID tags for automatic vehicle identification and authentication," *IEEE Trans. on Vehicular Technology* 54 (4), 1295-1303 (2005).
10. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, "Multiplexing encrypted data by using polarized light," *Opt. Commun.* 260, 109-112 (2006).
11. E. Tajahuerce, B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.* 39, 6595-6601 (2000).
12. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of IEEE* 91, 2021-2040 (2003).
13. S. Der, A. Chan, N. Nasrabadi, H. Kwon, "Automated vehicle detection in forward-looking infrared imagery," *Appl. Opt.* 43 (2), 333-348 (2004).
14. E. Pérez-Cabré, M.S. Millán, B. Javidi, "Visible and NIR spectral band combination to produce high security ID tags for automatic identification," *Proc. SPIE* 6394, 63940I, (2006).
15. M. S. Millán, E. Pérez-Cabré, B. Javidi, "Multifactor authentication reinforces optical security," *Opt. Lett.* 31, 712-723 (2006).
16. E. Pérez-Cabré, M.S. Millán, B. Javidi, "Design of distortion-invariant optical ID tags for remote identification and verification of objects," in *Physics of the automatic target recognition*, F. Sadjadi and B. Javidi, eds., Springer Verlag, 2007, Chap.12.
17. E. Pérez-Cabré, M. S. Millán, B. Javidi, "Remote optical ID tag recognition and verification using fully spatial phase multiplexing," *Proc. SPIE* 5986, 598602 (2005).
18. B. Javidi, "Nonlinear joint power spectrum based optical correlation," *Appl. Opt.,* 28 (12), 2358-2367 (1989).
19. E. Pérez, M. S. Millán, K. Chalasinska-Macukow, "Optical pattern recognition with adjustable sensitivity to shape and texture," *Opt. Commun.,* 202, 239-255 (2002).
20. *ATR Definitions and Performance Measures*, Automatic Target Recognizers Working Group (ATRWG) Publications, no. 86-001, 1986.
21. T. Kotzer, J. Rosen, J. Shamir, "Phase extraction pattern recognition," *Appl. Opt.* 31, 1126-1137 (1992).
22. E. Pérez, K. Chalasinska-Macukow, K. Styczynski, R. Kotynski, M.S. Millán, *Dual nonlinear correlator based on computer controlled joint transform processor: digital analysis and optical results*, J. Mod. Opt. 44, 1535-1552 (1997).